Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of Smart Grid Technology	))	GN Docket Nos. 09-47, 09-51, 09-137

Comments of AT&T Inc.—NBP Public Notice #2

Robert Vitanza
Gary L. Phillips
Paul K. Mancini

AT&T Inc.
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036
(202) 457-3076 – phone
(202) 457-3073 – facsimile

Its Attorneys

October 2, 2009

TABLE OF CONTENTS

I. INTRODUCTION..1

II. RESPONSES 6

1. **Suitability of Communications Technologies** 6

2. Availability of Communications Networks...24

3. Spectrum...26

4. Real Time Data...29

5. Home Area Networks. 31

III. CONCLUSION 33

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of Smart Grid Technology	)	GN Docket Nos. 09-47, 09-51, 09-137
	)	

COMMENTS OF AT&T INC.—NBP PUBLIC NOTICE #2

AT&T Inc., on behalf of itself and its affiliates ("AT&T"), respectfully submits these comments in response to the Commission's National Broadband Plan ("NBP") Public Notice #2, which seeks comments pertaining to the implementation of Smart Grid technology.[1]

I. INTRODUCTION

The Commission seeks comments on Smart Grid technology as part of its effort to support the development of the NBP. To assist the Commission in its fact gathering, AT&T will provide a summary of key issues associated with the implementation of Smart Grid technology into our nation's energy infrastructure, followed by more specific comments in response to the questions posed in NBP Public Notice #2.[2]

In the American Recovery and Reinvestment Act of 2009, Congress directed the Commission to include in the NBP "a plan for the use of broadband infrastructure and services in advancing . . . energy independence and efficiency."[3] President Obama has also declared that energy efficiency, energy independence, and reducing carbon emissions are necessary for

[1] Public Notice, Comment Sought on the Implementation of Smart Grid Technology, NBP Public Notice #2, GN Docket Nos. 09-47, 09-51, and 09-137, DA 09-2018 (rel. Sept. 4, 2009).

[2] AT&T has not responded to those questions that appear to be directed at utilities and consumers.

[3] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 6001(k)(2)(D), 123 Stat. 115 (2009) ("Recovery Act").

national security and economic stability.[4] The Recovery Act directive and the President's statement recognize that the nature of energy production and use in the United States must fundamentally change to overcome the critical issues resulting from dependence on foreign oil, the potential for detrimental climate change from fossil-based energy, and the challenges with meeting the ever growing demand for electric power. Energy conservation, and in particular the implementation of Smart Grid technologies, is a critical tool to move the United States forward on all of these issues while buying time for the development of new, more energy efficient technologies.

Smart Grid refers to the end result of updating the nation's electric transmission and distribution system with secure two-way communications capabilities that enable real-time interaction between utilities and their customers, more timely and complete information on the functional state of the grid, and greater access to renewable energy sources. Making the current grid smarter would be a critical enabler of energy efficiency. A mere five percent increase in grid efficiency would equate to energy savings equivalent to permanently eliminating the fuel and greenhouse gas emissions from 53 million cars.[5] Smart Grid enhancements will ease congestion and increase utilization of the electric grid, sending 50% to 300% more electricity through existing energy corridors.[6] These are just a couple of the benefits that a Smart Grid would bring in the first few years after implementation. In recognition of these benefits, the NBP should include policies that encourage the development and expansion of Smart Grid technologies in the most efficient and economical way.

---

[4] The White House, *Issues: Energy & Environment*, http://www.whitehouse.gov/issues/energy_and_environment/.

[5] *The Smart Grid: An Introduction, Exploring the Imperative of Revitalizing America's Electric Infrastructure*, prepared for the U.S. Department of Energy by Litos Stategic Communication, p. 7, *available at* http://www.oe.energy.gov/DocumentsandMedia/DOE_ SG_Book_Single_Pages(1).pdf ("*Smart Grid Introduction*").

[6] Id. at p. 17.

The following attributes are fundamental components of a fully implemented Smart Grid:

- Enables active customer participation;
- Accommodates all generation and storage options;
- Enables new products, services, and markets;
- Provides the power quality for the range of needs in the 21st century;
- Optimizes asset utilization and operates efficiently;
- Addresses disturbances – automated prevention, containment, and restoration; and
- Operates resiliently against physical and cyber attacks and natural disasters.[7]

To achieve these attributes, the National Institute of Standards and Technology ("NIST") has been charged with identifying and evaluating existing Smart Grid standards, measurement methods, and technologies and filling any gaps in those standards, methods and technologies and in other support services needed for Smart Grid adoption.[8] NIST is currently undertaking this charge as part of its Smart Grid Roadmap process.[9] AT&T encourages the Commission to take an active role in coordinating with NIST to ensure that the Commission's actions and policies pertaining to the implementation of Smart Grid technology are consistent with the standards being developed by NIST and that those actions and policies provide clear guidance to providers of Smart Grid equipment and services.

---

[7] *The Modern Grid Strategy, The Principal Characteristics*, Department of Energy website, *available at* http://www.netl.doe.gov/moderngrid/characteristics.html; *Smart Grid Introduction*, p. 38.

[8] The Energy Independence and Security Act of 2007 grants NIST, an agency of the United States Department of Commerce, "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." Energy Independence and Security Act of 2007, Pub. L. 110-140, Sec. 1305(a), 121 Stat. 1492 (2007).

[9] At the request of NIST and the Electric Power Research Institute, the IEEE P2030 group was formed to help identify gaps in current Smart Grid standards and to craft standards to fill those gaps. IEEE P2030 is broken into three task forces: TF1 works on the functions and infrastructure of the Smart Grid, TF2 works on the data models associated with information transactions, and TF3 works on the communications infrastructure to support information transactions.

The Smart Grid network should be interoperable and based on the Internet Protocol ("IP") standard. IP is a recognized international standard for data networking and data communications and is readily supported by both wireless and wireline commercial communications operators. Its use permits flexible equipment and system configuration and secure data connections for customers using the IP protocol. Further, Congress has expressed an intention to enable IP-based networks for Smart Grid demonstration projects.[10] By ensuring interoperable communication and coordination across inter-system interfaces with IP-based networks, the Commission will enable resources to be spent only on services and technologies that are compatible with other systems and that will not soon become obsolete.

In the Recovery Act, Congress directed that the NBP should address the "most effective and efficient mechanisms for ensuring broadband access"[11] and include a strategy to achieve "maximum utilization of broadband infrastructure and service by the public."[12] To that end, the NBP should encourage the use of existing commercial communications networks and services to support Smart Grid deployment. Effective and efficient Smart Grid implementation requires a coordinated, collaborative effort between electric utilities and commercial communications operators. Such a partnership would allow utilities and consumers to maximize the utilization of already deployed and capable network infrastructure, while quickening the pace of sound Smart Grid deployment in a cost effective manner.

---

[10] Recovery Act, Sec. 405(3), amending Section 1304(b)(3) of Title XIII of the Energy Independence and Security Act of 2007 (42 U.S.C. §17381) to add subpart (F) ("The Secretary shall require as a condition of receiving funding under this subsection that demonstration projects utilize open protocols and standards (including Internet-based protocols and standards) if available and appropriate.").

[11] Recovery Act, Sec. 6001(k)(2)(A).

[12] Recovery Act, Sec. 6001(k)(2)(B).

Commercial communications operators offer reliable, robust and nearly ubiquitous, secure network capabilities and services. To the extent that a utility requires expanded coverage or enhanced network performance not presently available from the services commercial communications operators offer to consumers, utilities can negotiate service level agreements with commercial communications operators to facilitate the expansion of network coverage or to obtain guarantees of enhanced network performance, such as through the use of managed services. Commercial communications operators will be incented to negotiate service level agreements to make the enhancements sought by utilities to secure the Smart Grid business, as well as to derive incremental benefits from expanded consumer sales.

Of course, the use of commercial communications networks need not be to the exclusion of utility-owned assets. Utilities with existing communications systems can utilize commercial communications networks and managed services offered by commercial communications operators to augment the capabilities of their existing systems. At the same time, cybersecurity must be a priority of any Smart Grid network to protect the secure nature of communications transiting the network. Commercial communications operators have a demonstrated record of incorporating robust cybersecurity capabilities into their networks. The NBP should encourage utilities to leverage this expertise by partnering with commercial communications operators in the development of Smart Grid systems.

In all events, unreasonable network management rules that restrict a commercial communications operator's ability to effectively manage network communications could hamper efforts to deliver a cost effective, interoperable and secure Smart Grid. The NBP should recognize the ability of commercial communications operators to manage network traffic to ensure effective routing of Smart Grid data.

II. RESPONSES

1. Suitability of Communications Technologies

a. What are the specific network requirements for each application in the grid (e.g., latency, bandwidth, reliability, coverage, others)? If these differ by application, how do they differ?

Comments: The Smart Grid is not a one time implementation of technology into the electric grid but rather the application of advanced information and telecommunications technologies (both wireline and wireless) to the utilities industry over a period of time. Consequently, the Smart Grid will evolve over the next few years (or perhaps decades) to encompass many different aspects and business processes of the utilities industry and the household management of energy usage. The specific network requirements for each application will differ and evolve over time.[13]

Today, Smart Grid deployments are focused on Advanced Metering Infrastructure ("AMI"), which typically involves the installation of smart meters at the customer premises. Although it has been estimated that AMI comprises only about 4.7% of all electric meters,[14] its use is growing. AMI allows utilities to remotely monitor electrical usage, thus reducing the operational expenses associated with reading meters. AMI also allows utilities to detect problems in the electric grid, such as might occur when a cluster of homes ceases consuming electricity, thereby allowing faster trouble recognition, isolation and restoral. It also potentially

[13] The Smart Grid is not one system, but a series of network systems. The applications that are needed within each system will differ depending on the needs of the particular utility.

[14] *See* Statement of Patricia Hoffman, Acting Assistant Secretary of Electricity Delivery and Energy Reliability, Department of Energy before the Subcommittee on Energy and Environment, Committee on Science and Technology, U.S. House of Representatives, p. 2 (July 23, 2009), *available at* www.congressional.energy.gov/documents/7-23-09_Final_Testimony_(Hoffman).pdf.

allows utilities to communicate usage information to customers, who can alter energy use behavior. Using AMI, consumers can use electricity more efficiently and utilities can operate the electric grid more efficiently.[15]

AMI is a prerequisite to a fully functional Smart Grid. Presently, AMI data and bandwidth requirements are low – a few hundreds of bytes per second for individual meters in point to point configurations[16] to a few thousands of bytes per second for concentrators and access control points in mesh topology networks.[17] Those requirements are easily met by today's commercial communications networks. While it is true that over the next few years, more advanced and demanding applications will be incorporated into the Smart Grid, the capabilities of commercial communications networks will likewise expand at a rapid pace. See AT&T's response to Question 1.d. pertaining to the evolution of networks. Among the most promising applications of tomorrow are the following:

- "Demand response" applications associated with home area networks that will allow consumers to reduce energy use during times of peak demand (or shift energy use to times of off-peak demand);
- Remote meter disconnect applications that allow utilities to remotely disconnect service after a customer moves;

[15] *See Smart Grid Introduction*, p. 11.

[16] A point to point network configuration allows a direct connection between the smart meters, which are installed with modems and SIM cards, and the utility.

[17] A mesh network configuration involves an indirect connection with the utility whereby the smart meters are connected to each other and transmit data to a local collection point, which forwards the data to the utility.

- Fault isolation applications that allow a utility to isolate a service area "downstream" from a downed power line or other grid deficiency and reroute electricity around the problem;
- Mobile energy transaction applications that allow consumers to connect an electric vehicle to a remote charging station away from home and utilities to appropriately bill for the energy used or credit for the energy discharged into the grid during that connection; and
- Utility infrastructure management and control applications that allow utilities to more extensively automate electric grid infrastructure operations.[18]

The communications network requirements for each of these applications are not definitively established, as the NIST Smart Grid Roadmap process, where application requirements will be mapped to standards, is in the initial stages.[19] Compared to current AMI applications, some future applications, such as those used for utility infrastructure management and control, may demand greater bandwidth and higher network performance, whereas other applications, such as those used for demand response, remote meter disconnect, fault isolation, and mobile energy transactions, may operate adequately with bandwidth and network performance characteristics that are similar to today's applications.

Regardless of the specific applications that are adopted, it is expected that over time Smart Grid networks in the aggregate will demand greater bandwidth, lower latency, and enhanced reliability. To accommodate these requirements, the communications network

---

[18] For example, voltage measurement and control applications will allow utilities to monitor voltage variability on a real-time basis, from which a utility can optimize the distribution of energy within the electric grid and potentially significantly reduce costs associated with peak electricity demands.

[19] IEEE P2030 was formed on June 3, 2009. The next plenary meeting will be held October 27-29, 2009.

supporting the Smart Grid must be highly adaptable, with a heavy emphasis on scalability, flexibility, and backwards compatibility. Utilities will also need to carefully evaluate data processing requirements because data transmission and storage requirements will likely grow exponentially as Smart Grid applications proliferate in the network.

b. Which communications technologies and networks meet these requirements? Which are best suited for Smart Grid applications? If this varies by application, why does it vary and in what way? What are the relative costs and performance benefits of different communications technologies for different applications?

Comments: As discussed in response to Question 1.a., the recently initiated NIST Smart Grid Roadmap process and the lack of mature Smart Grid technology limits AT&T's response to this question as it applies to specific applications.

Generally, Smart Grid networks are configured with either a point to point topography or mesh topography. A point to point network consists of direct connections between the smart meters and the utility, typically by incorporating a modem and SIM card, via a commercial wireless network. Conversely, a mesh network configuration involves an indirect connection with the utility whereby smart meters transmit data to a centrally located hub directly or via one or more neighboring meters. In a mesh network, connectivity between smart meters and the hub typically occurs over a utility owned and operated dedicated network, whereas backhaul from the hub to the utility may transit over a commercial communications network. Although mesh networks and point to point networks can both meet the performance requirements of current Smart Grid applications, a point to point architecture allows utilities to leverage existing the infrastructure and capabilities of commercial communications networks rather than incur the significant cost of building a dedicated, single use mesh network.

The common thread running through many of the fundamental attributes of a Smart Grid, as listed above, is the idea that the technology must be flexible enough to accommodate evolving devices and applications. In other words, Smart Grid technologies must be able to adapt to meet the needs of future Smart Grid applications without significantly disrupting existing applications. Here, interoperable advanced IP-based networks utilized by commercial communications operators are the most effective way for the Smart Grid to evolve while minimizing the risks of technical obsolescence. The interoperable nature of an IP-based network was succinctly stated in a study conducted by the Worldwide Consortium for the Grid on the state of commercial wireless infrastructure:

> The ultimate glue and interoperability answer for the future is IP. . . . [T]o ensure true interoperability and compatibility with future technologies, IP-based products and networks require an increasing emphasis for all technology and procurement decisions by DoD. [20]

Congress has also endorsed the IP standard as sufficient to warrant funding for Smart Grid demonstration programs.[21]

IP-based networks have substantial advantages. First, IP-based networks scale flexibly to accommodate new connections and adapt rapidly to changing load – a capability critical to Smart Grid evolution. Second, IP enables applications to communicate flexibly regardless of the underlying physical infrastructure of the network. If the commercial communications operator can accept and deliver IP packets at its network edge (*i.e.*, conforms to IP/OSI Layer 3), the

[20] Diaz, *Final Report on Utility of Commercial Wireless Study: A Technology Roadmap for Disaster Response*, Worldwide Consortium for the Grid, p. 9 (Nov. 2006), *available at* http://www.nav6tf.org/documents/utility_of_commercial_wireless_study_disaster_relief_final_report.pdf ("*W2COG Report*").

[21] Recovery Act, Sec, 405(3).

underlying protocols used by that commercial communications operator are largely irrelevant. Third, the ability of IP networks to self-heal is inherent in the technology.[22] If a transmission link fails, the network will automatically take steps to avoid the failed element and deliver the communications. This capability will ensure a reliable Smart Grid communication infrastructure. Fourth, the interoperable nature of IP networks minimizes cost. And, fifth, IP networks enhance the cybersecurity tools available to combat unauthorized access to a network, as the acceptance of IP networking as the worldwide standard for inter-networking communications has resulted in a global ecosystem of security applications for use with those networks.

AT&T encourages the Commission to ensure that the NBP emphasizes interoperability that does not constrain investment and innovation. The IP protocol is ideally suited in this respect because it allows for loose coupling between the physical communications network and the applications used on that network. This allows applications to evolve with assurance that they can communicate across any IP-based network. Likewise, it assures that the underlying network can expand and introduce enhanced performance without adverse impact to applications. Such interoperability supported by the IP protocol and IP networking will ensure that resources are spent only on services and technologies that are compatible with other systems and reduce the risk of technical obsolescence. The Commission should take an active role in coordinating with the Federal Energy Regulatory Commission ("FERC") and NIST to ensure that Commission action or policies pertaining to Smart Grid technology are implemented in a manner that is consistent with the interoperability standards under consideration by NIST.

---

[22] *See* National Energy Technology Laboratory, *A Vision for the Modern Grid*, United States Department of Energy, pp. 4-5 (March 2007), *available at* http://www.netl.doe.gov/moderngrid/docs/A%20Vision%20for%20the%20 Modern%20Grid_Final_v1_0.pdf.

c. What types of network technologies are most commonly used in Smart Grid applications?

Comments: Only recently have utilities and business users started implementing Smart Grid solutions. Thus, it is difficult to say which network technologies are most common. See the Introduction and AT&T's response to Question 1.b. regarding different technologies that are used and should be used with Smart Grid networks. Yet, one category of networks commonly used in Smart Grid deployments is commercial communications networks. See AT&T's response to Questions 1.d and 1.e. for a complete discussion of the benefits of using commercial communications networks to support Smart Grid implementation.

d. Are current commercial communications networks adequate for deploying Smart Grid applications? If not, what are specific examples of the ways in which current networks are inadequate? How could current networks be improved to make them adequate, and at what cost? If this adequacy varies by application, why does it vary and in what way?

Comments: Yes, today's commercial communications networks are adequate to support the deployment of current Smart Grid technology and will adequately support the Smart Grid applications in the foreseeable future. The demands of a Smart Grid are not unique. In fact, commercial communications operators already support Smart Grid applications for electric utilities and business customers with the network performance attributes sought by those customers.

AT&T's wireless network, for example, currently supports SmartSynch's Smart Grid solution, which allows electric utilities to remotely monitor electric meters.[23] Texas-New Mexico Power ("TNMP") recently selected the SmartSynch/AT&T SmartMeter™ solution for a 10,000 unit point-to-point trial deployment to residential customers in TNMP's service area.[24] An end-user customer, the State of Mississippi, likewise chose to install SmartSynch/AT&T meters in public buildings to improve energy efficiency.[25] AT&T's wireless network also supports Cooper Power Systems outage monitors and voltage sensors,[26] as well as Itron's OpenWay® local-area networking, which gives utilities two-way communications for access to data from meters throughout their systems.[27] Likewise, other commercial communications operators are facilitating Smart Grid implementation over their existing networks.[28]

Not only do commercial communications networks currently support the Smart Grid, they are the best method to support the Smart Grid now and for the foreseeable future. Achieving a fully-interoperable Smart Grid is an enormous task, and more rapid progress will be

---

[23] *See* Narayan Bhat, *With SmartSynch, AT&T Offers Smart Grid Technology To Utility Companies*, TMCnet.com (March 24, 2009), *available at* http://telecom-expense-management-solutions.tmcnet.com/topics/enterprise-mobile-communications/articles/52879-with-smartsynch-att-offers-smart-grid-technology-utility.htm ("SmartSynch Offer"). SmartSynch reports that its smart grid solution is deployed at more than 100 utilities throughout North America. *Id*.

[24] PRNewswire via COMTEX, *Texas-New Mexico Power Selects SmartSynch/AT&T Solution for 10,000 Unit Point-to-Point SmartMeter™ Trial Deployment Throughout Texas Market*, IT.TMCNET.com (April 16, 2009), *available at* http://it.tmcnet.com/news/2009/04/16/4136751.htm.

[25] Press Release, *SmartSynch Awarded State Energy Program Grant*, Mississippi Development Authority (Aug. 20, 2009), *available at* http://www.mississippi.org/index.php?id=719.

[26] *See* Jeff St. John, *AT&T Links Cooper Power Systems' Smart Grid Devices*, greentechgrid (June 25, 2009), *available at* http://www.greentechmedia.com/articles/read/att-links-cooper-power-systems-smart-grid-devices/.

[27] Press Release, *AT&T Powers AMI Platform from Itron* (Aug. 18, 2008), *available at* http://www.itron.com/pages/news_press_individual.asp?id=itr_016767.xml.

[28] *See e.g.* Jeff St. John, *Verizon, Itron Hook Up to Offer Smart Grid Communications*, Seeking Alpha (April 2, 2009), *available at* http://seekingalpha.com/article/129114-verizon-itron-hook-up-to-offer-smart-grid-communications; Marguerite Reardon, *T-Mobile Goes for Smart Grids*, CNET News (April 23, 2009), *available at* http://news.cnet.com/8301-1035_3-10226418-94.html.

made if there is more collaboration between utilities and commercial communications providers when deploying Smart Grid infrastructure. Such an approach would minimize the risks of stranded costs and obsolescence and maximize efficient development of a Smart Grid. Congress has recognized these benefits, as it requires that the NBP achieve "maximum utilization of broadband infrastructure and service."[29] The Worldwide Consortium for the Grid similarly concludes that a collaborative approach works best for an interoperable national network:

> [N]o one US government agency, no one single vendor and no single program can achieve communications systems interoperability on its own. Interoperability should be considered a multi-stakeholder goal requiring an integrated vision and cooperative strategy.[30]

Utilities excel at supplying energy to the nation, whereas commercial communications operators are proficient at facilitating the communication of information. The nation should harness those proficiencies to facilitate the deployment of Smart Grid technologies. Any rationale for building a dedicated single use network instead of using a commercial communications network is not justified by the significant costs of that endeavor. While there may not be a consensus on the exact cost to build and operate a dedicated single use network for the Smart Grid, there should be no doubt that the costs will be significant.[31] Utilities that leverage the existing infrastructure and expertise of commercial communications operators

[29] Recovery Act, Sec. 6001(k)(2)(B).

[30] *W2COG Report*, p. 9.

[31] For comparison, it is estimated that the cost of building and operating a national data only network for public safety will be approximately $10.4 billion. *See* Ryan Hallahan, Jon Peha, *Quantifying the Costs of a Nationwide Broadband Public Safety Wireless Network*, 36th Telecommunications Policy Research Conference, p. 34 (Sept. 2008), *available at* http://www.ece.cmu.edu/~peha/costs_of_public_safety_network.pdf.

would bear only a portion of those eventual costs versus 100% of the costs associated with a greenfield build.[32]

Certain utilities have argued that commercial communications networks cannot meet utility Smart Grid demands due to issues associated with coverage, reliability, security, and emergency preparedness and recovery. In fact, with respect to each of these attributes, commercial communications networks can and do have sufficient capabilities to meet the demands of the Smart Grid today and in the foreseeable future, while offering the best chance for its timely development at an economical cost.

Coverage: Commercial communications operators are experienced in rapidly scaling and expanding both wireline and wireless network capacity to meet the needs of large customer bases. For example, commercial communications operators have managed the increase in wireless customers from less than 100 million in 2000[33] to over 270 million as of December 2008.[34] Commercial communications operators had deployed over 240,000 cell sites across the country[35] and at least three commercial communications operators provide wireless service in census blocks that cover more than 95 percent of the U.S. population.[36] This coverage should

---

[32] The purchasing power that commercial communications operators derive from their large base of users also reduces equipment costs, to the benefit of utilities using commercial communications networks for Smart Grid deployments.

[33] *History of Wireless Communications, From Building the Wireless Future to Expanding the Wireless Frontier*, CTIA Website, *available at* http://www.ctia.org/media/industry_info/index.cfm/AID/10392.

[34] Press Release, *CTIA – The Wireless Association® Announces Semi-Annual Wireless Industry Survey Results* CTIA website (April 1, 2009), *available at* http://www.ctia.org/media/press/body.cfm/prid/1811.

[35] Ex Parte Letter from Christopher Guttman-McCabe to Chairman Julius Genachowski (July 9, 2009), *available at* http://files.ctia.org/pdf/filings/2009_Wireless_Economic_Contributions.Letter.Final.pdf ("CTIA Ex Parte").

[36] *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Radio Services*, WT Docket No. 08-27, Thirteenth Report, DA 09-54, p. 5 (rel. Jan. 16, 2009) ("*Thirteenth CMRS Competition Report*").

allow commercial communications operators to provide Smart Grid services in most areas of the United States.

Moreover, commercial communications operators are continuing to invest in their networks. For example, AT&T plans to invest another $17 to $18 billion more this year in its wireless and wireline infrastructure.[37] In the process, nearly 2,000 cell sites will be added to expand coverage to new cities and improve coverage in existing areas. By relying on commercial communications networks, utilities will benefit from this expanded coverage, driven by both the utilities' needs and the needs of hundreds of millions of other commercial customers.

Commercial communications operators can also expand their network coverage to meet the needs of a particular utility, or augment coverage with satellite service. For example, AT&T has partnered with satellite service provider TerreStar Networks to offer back-up satellite service where terrestrial wireless service is unavailable in an integrated mobile device. This solution can be adapted to Smart Grid use and is well-suited for energy and utility users.[38]

Commercial communications operators also maintain the ability to scale their networks to meet rising demand in an emergency or other expected situation. Commercial communications operators have the ability to deploy mobile equipment to recover or increase network capacity following a disaster, including self-sufficient temporary cell sites and network offices that can be used while a damaged site or office is repaired or rebuilt. In emergencies, the mobile equipment can be used to provide wireless communications capabilities, including satellite communications,

---

[37] Press Release, *AT&T to Invest More Than $17 Billion in 2009 to Drive Economic Growth* (March 10, 2009), *available at* http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=26597.

[38] AT&T's expects its Integrated Cellular-Satellite Solution to be available in the first quarter of 2010. More information on AT&T's Integrated Cellular-Satellite Solution is available at http://www.wireless.att.com/ businesscenter/business-programs/government/solutions/integrated-cellular-satellite-solution.jsp.

to support the recovery efforts of first responder organizations, local emergency operations centers, government agencies and commercial communications networks.

The history of consumer adoption of advanced communications capabilities and of commercial communications operators scaling their networks to meet those demands demonstrates that commercial communications operators could effectively manage an increase in usage due to Smart Grid applications.

Performance: As demonstrated in the examples above, existing commercial communications networks already support current Smart Grid applications. AT&T's networks are capable of reliably supporting current and foreseeable future Smart Grid applications, whether a utility's needs dictate a wireline connection, wireless connection, or managed services.

With the evolution of its wireless network to HSPA 7.2 and later LTE, AT&T is upgrading its wireless network to meet future performance needs. HSPA 7.2 and LTE are ideally suited to Smart Grid application due to high spectrum efficiency, high data rates, and low latency, without compromising security. A recent 3G Americas White Paper that, in part, studied downlink performance of a European HSPA 7.2 network, documented average downlink speeds of nearly 2 Mbps, and peak downlink speeds of up to 3.8 Mbps in good coverage.[39] HSPA 7.2 latency has been estimated between 50 and 100 milliseconds, depending on the data and network conditions.[40] With respect to both, speed and latency, HSPA 7.2 network performance exceeds the currently defined needs of Smart Grid devices and applications.

---

[39] Peter Rysavy, *HSPA to LTE-Advanced: 3GPP Broadband Evolution to IMT-Advanced (4G)*, 3G Americas, p. 45 (Sept. 2009), *available at* http://www.rysavy.com/Articles/2009_09_3G_Americas_RysavyResearch_HSPA-LTE_Advanced.pdf ("*Rysavy, HSPA to LTE-Advanced*")..

[40] *3G LTE Tutorial – 3GPP Long Term Evolution*, radioELECTRONICS.com, *available at* http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/3g-lte-basics.php.

AT&T plans to begin LTE network deployments in 2011, while many other commercial communications operators have also announced plans to deploy LTE networks in the near future.[41] LTE technology will facilitate even higher spectral efficiency and data rates and lower latency than HSPA 7.2. LTE is expected to hit peak downlink speeds of 100 Mbps and peak uplink speeds of 50 Mbps, with latency ranging from approximately 10 milliseconds to less than 100 milliseconds.[42] While latency depends on many factors, there is no escaping the fact that commercial communications networks meet the needs of current Smart Grid applications and as networks evolve, latency is trending downward:

> Each successive data technology from GPRS forward reduces latency, with HSDPA networks having latency as low as 70 milliseconds (msec). HSUPA brings latency down even further, as will 3GPP LTE. Ongoing improvements in each technology mean all these values will go down as vendors and operators fine tune their systems.[43]

The superior network performance of an LTE network also translates into a cost effective network. It is estimated that a LTE network with average data rates of 5 to 10 Mbps will translate into a cost per megabyte that is substantially lower than the cost of previous network technologies.[44] These reduced costs for commercial communications operators will translate into lower overall costs for utilities that construct a Smart Grid in partnership with commercial communications operators.

---

[41] Other carriers' LTE plans can be accessed at the following websites: Verizon - http://news.vzw.com/news/2009/02/pr2009-02-18.html; T-Mobile - http://www.4ginfo.com/index.php/t-mobile-makes-honest-predictions-for-lte.html; MetroPCS – http://gigaom.com/2009/03/03/metropcs-wants-to-deploy-lte-in-2010/; Century Tel-Embarq - http://www.lteconference.com/newt/l/networkevolution/lte08/article_view.html?artid=20017635836.

[42] *Rysavy, HSPA to LTE-Advanced*, p. 51; *See also 3GPP TR 25.913*, *Technical Report*, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN) (Release 8), Sec. 6 (Dec. 2008), *available at* http://www.3gpp.org/ftp/Specs/archive/25_series/25.913/.

[43] *Rysavy, HSPA to LTE-Advanced*, p. 50.

[44] Martin Reitenspieß, Peter Weichsel, Niels Rosenhäger, *LTE: Delivering the Future of Wireless*, p.2 (2009), *available at* http://www.booz.com/media/uploads/LTE_Delivering_Future_of_Wireless.pdf.

Although network performance for supporting a Smart Grid often focuses on network connectivity over the commercial wireless network, the network configuration followed should reflect the needs of the utility, which may be best supported by a wired broadband connection or by secure managed services. AT&T offers a range of secure managed service capabilities that can foreclose exchanges with other networks, such as the public switched telephone network or the public Internet, and enhance network security. For example, AT&T's enhanced virtual private network services ("VPNs"), which validates that communications between points on the network are authorized, allows customers to receive differentiated service handling that will enhance aspects of network performance for that customer.

Security: Commercial communications networks offer sophisticated cybersecurity protections that are fully capably of supporting Smart Grid technologies. Many commercial providers have extensive experience in developing comprehensive security solutions for complex network environments based on their unique vantage points in the communications industry. Network exploits, malware, flooding attacks, protocol anomalies and other threats are generally visible and often abundant on the Internet and commercial communications operators often have the ability to identify and mitigate them long before they have any significant affect on enterprise security. Thus, whereas a communications network operated by a utility company may only see the immediate attacks directed against it, commercial communications operators with birds-eye views of the global Internet are typically better positioned to recognize broader, emerging threat trends and to take action before those threats cause significant harm.

AT&T, for example, maintains a substantial cybersecurity program, and expects that other commercial communications operators have adopted their own programs to protect network security. AT&T is uniquely positioned to understand those threats on the Internet with capabilities that include being the largest provider of Internet services; operating a global IP network footprint; using an Internet data analysis platform to examine threats; maintaining a team that operates 24 x 7 to assess any significant activities on the Internet that could affect network services; maintaining an algorithm research team that investigates and tests methods for automated detection of network threats; and participating in the security and networking research communities.

The size and scope of AT&T's global network, coupled with its cyber-security capabilities, gives it a unique perspective into malicious cyber-activity. AT&T's advanced network technology currently transports more than 17 Petabytes of IP data traffic each day and that load is expected to double every 18 months for the foreseeable future. Utilities may find this extensive cybersecurity expertise helpful in addressing their own security needs.

AT&T also has made significant investments in the security of its wireless network. AT&T's wireless network complies with 3GPP airlink security standards and uses secure protocols in order to maintain and manage communication with the mobile station. Encryption further protects both user data and network control information. Following authentication and key agreement, the network and end-user equipment uses a 128-bit key and strong encryption algorithms. Significant resources have also been invested in the AT&T core mobility and wide area network area in order to comply with and exceed industry security standards.

AT&T's wireline and wireless networks are supported by a comprehensive global security organization comprised of over 700 security professionals. This organization is dedicated to the physical and logical security of the AT&T global network and its service offerings. The AT&T global security organization reviews and assesses AT&T's security control posture to keep pace with industry security developments and to satisfy regulatory and business requirements. AT&T actively participates in a number of global security organizations, and maintains a comprehensive set of security standards based in part on similar leading industry standards (COBIT, ISO/IEC 27001:2005, etc.). Given the dynamic communications networks that AT&T supports, the library of AT&T security standards is continually re-evaluated and modified as industry standards evolve and as circumstances require.

Emergency Preparedness and Recovery. Commercial communications operators have invested millions of dollars to maximize the effectiveness of their networks in the event of an emergency. Although no network, including a dedicated single use network, is invulnerable to the most severe catastrophes, commercial communications operators have developed programs and emergency infrastructure to minimize disaster exposure and minimize downtime where a disaster or other unexpected event affects service quality. As an example, AT&T has invested over $500 million in its network disaster recovery program. This program insures network reliability by harnessing the following assets, among others:

- Specially-designed semi-tractor trailers strategically located around the U.S. that can be dispatched as needed to act as a virtual network office;
- Mobile command centers that provide emergency response teams with fully-equipped and controlled office space in the event of a disaster and can be rapidly deployed and set up at a recovery site;
- Self-contained mobile cell sites (i.e. cells on wheels ("COWs") and cells on light trucks ("COLTs")) to replace a failed cell site or supplement cellular capacity during times of increased demand;
- Emergency communications vehicles ("ECV"), which use a satellite link to provide command communications during the initial phase of a recovery effort;

- Emergency equipment located at designated locations, such as portable generators, chillers, pumps and fuel cells placed at network offices deemed at risk and permanent generators and battery backup at all wireless switches and many cell sites; and
- Managers, engineers and technicians who are trained in network recovery and participate in periodic recovery exercises to insure they are prepared when disasters occur.[45]

These types of efforts, among others, prepare commercial communications networks for inevitable disasters and minimize the opportunities for long-term network reliability problems when disasters occur. As a commercial communications operator with nationwide operations, AT&T can direct its emergency response resources to the geographic area affected. It would be inefficient and exorbitantly expensive for every utility to attempt to implement such extensive emergency protection and recovery capabilities for their dedicated single use network.

In sum, commercial communications networks offer all of the features needed for a fully operational Smart Grid —coverage, performance, security, and emergency preparedness and response. It would be difficult, if not impossible, for a utility to economically and comprehensively replicate these features in a dedicated single use network. Of course, it is unrealistic to expect each commercial communications operator to cover 100% of the nation's electric grid infrastructure or to achieve the highest performance metrics in every corner of its network today. The same is true of dedicated single use networks. But to the extent that a utility customer seeks more expansive coverage or enhanced performance or security, the utility and

[45] Information about AT&T's disaster recovery programs is available at http://www.corp.att.com/ndr/.

commercial communications operator can enter into a service level agreement to provide for those improvements.

By collaborating, utilities and commercial communications operators can achieve quicker and more economical full Smart Grid deployment. However, for those utilities that own and operate existing emergency response systems, commercial communications networks need not always supplant those networks. Where a utility has an existing network that meets the utility's current needs, the utility should still explore the use of commercial communications networks as a strategy to cost-effectively meet emerging Smart Grid needs. At the same time, it is not prudent to assume that older existing systems can be enhanced and expanded to meet Smart Grid needs in a cost effective manner.

e. How reliable are commercial wireless networks for carrying Smart Grid data (both in last-mile and backhaul applications)? Are commercial wireless networks suitable for critical electricity equipment control communications? How reliably can commercial wireless networks transmit Smart Grid data during and after emergency events? What could be done to make commercial wireless networks more reliable for Smart Grid applications during such events?

Comments: Commercial communications networks possess the reliability required to support any application needed for the Smart Grid. Smart Grid applications are not unique compared to the network demands in other industries – in terms of bandwidth, performance or reliability. Yet, commercial communications networks have met those demands, even for industries that rely on communications in life and death situations. For example, the Worldwide

Consortium for the Grid considers commercial communications networks sufficiently reliable to support first responders in disaster response situations:

> There exist mature and pervasive Wireless Wide Area Network (WWAN) cellular service in practically every perceivable disaster area in the US and Canada. Assuming that the basic power and site infrastructure remains intact, the service providers will continue to provide a ***reliable service*** and opportunity to utilize a growing array of devices (handhelds, smartphones, laptops, cellular modem backhaul on WLAN equipment, etc.) readily available in the commercial sector.[46]

If commercial communications networks are reliable enough for first responders, they are certainly sufficient for Smart Grid applications.

In fact, current Smart Grid applications generally require minimal bandwidth and latency requirements. In contrast, commercial communications operators capably serve the needs of many government and business customers that demand high bandwidth, low latency and otherwise high network performance attributes.

See AT&T's response to Questions 1.d. for a more thorough discussion of the reliability of commercial communications networks.

2. Availability of Communications Networks.

a. What percentage of electric substations, other key control infrastructure, and potential Smart Grid communications nodes have no access to suitable communications networks? What constitutes suitable communications networks for different types of control Infrastructure? We welcome detailed analyses of substation and control infrastructure connectivity, potential connectivity gaps, and the cost-benefit of different alternatives to close potential gaps.

---

[46] *W2COG Report*, p. 8 (emphasis added).

Comments: In light of the ubiquity of the communications infrastructure in the United States, AT&T believes that it is highly likely that access to effective communications is available at the vast majority of key installations that compose the electric grid. Commercial wireless operators alone operate over 240,000 cell sites across the country[47] and provide wireless service in census blocks that cover more than 99.6 percent of the U.S. population.[48] Further, some utilities have existing private networks, though it is not safe to assume that those networks can accommodate a significant Smart Grid deployment. To the extent that a utility requires expanded coverage, utilities can negotiate with commercial communications operators to provide that coverage.

The remaining questions are being thoroughly explored by NIST through the Smart Grid Roadmap process. AT&T encourages the Commission to rely upon and, as appropriate, coordinate with NIST regarding the standards process rather than undertaking a separate process that might cause contradiction and confusion.

b. What percentage of homes have no access to suitable communications networks for Smart Grid applications (either for last-mile, or aggregation point connectivity)?

Comments: See AT&T response to Questions 1.d. and 2.a. regarding population covered by wireless connectivity.

[47] CTIA Ex Parte Letter.

[48] *Thirteenth CMRS Competition Report*, p. 5.

c. In areas where suitable communications networks exist, are there other impediments preventing the use of these networks for Smart Grid communications?

Comments: To the extent that organizations or governments enact policies that promote the allocation of spectrum dedicated solely for the use of utilities or the building of single-use utility networks, those policies may have the effect of delaying the implementation of Smart Grid technologies into the electric grid. As discussed above, commercial communications operators are typically best positioned to put spectrum into use quickly and cost-effectively in a manner that supports the Recovery Act's goal of "maximum utilization" of broadband infrastructure.

d. How does the availability of a suitable broadband network (wireless, wireline or other) impact the cost of deploying Smart Grid applications in a particular geographical area? In areas with no existing networks, is this a major barrier to Smart Grid deployment?

Comments: As discussed more fully in AT&T's response to Question 1.d., commercial communications networks offer a more cost-effective and expedient alternative to single-use networks deployed by electric utilities.

3. Spectrum.

a. How widely used is licensed spectrum for Smart Grid applications (utility-owned, leased, or vendor-operated)? For which applications is this spectrum used?

Comments: In response to Question 1.d., AT&T provides information on the current use of commercial wireless networks for certain Smart Grid applications. The licensed spectrum used for this connectivity is in the cellular 850 MHz and PCS 1900 MHz ranges. Commercial wireless carriers have announced plans to deploy 4G networks on 700 MHz and 2100 MHz frequencies, which may also be used for Smart Grid applications.

The use of licensed spectrum offers several advantages to utilities and Smart Grid applications, including protection against interference and enhanced penetration and propagation – particularly in lower spectrum ranges. Utilities deploying dedicated single use networks can experience interference, coverage, and propagation challenges because they are typically deployed using 2400 MHz shared unlicensed spectrum. These challenges can affect the location and number of access points and concentrators, and thus, the ultimate cost of a network build. For example, limited or no obstacles might allow a network design with ratios of several thousand devices to one concentrator, while significant interference might require a design with only a few dozen devices per concentrator. Further, because the potential for interference to systems using unlicensed spectrum is not static, it requires constant monitoring and may require retuning of the deployed network configuration.

Using commercially licensed spectrum for Smart Grid applications also is the most efficient use of spectrum, as it allows for the greatest number of users over a limited spectrum resource. The use of existing commercially licensed spectrum also allows for the rapid addition of new meters/sensors to the Smart Grid (i.e., it is scalable), and for reduced unit costs for all parties, as the high fixed cost of the wireless network are shared amongst the largest customer base possible. Utility use of commercial communications networks also acts as an incentive for commercial communications operators to expand their networks into unserved areas due to the incrementally improved business case of having both Smart Grid application demand (particularly meters and sensors) coupled with consumer demand for wireless broadband and mobility services.

e. Are current spectrum bands currently used by power utilities enough to meet the needs of Smart Grid communications?

Comments: It is unlikely that current spectrum allocated to electric utilities is sufficient to address the future needs of the Smart Grid and do so for all electric utilities. However, a negative answer to this question does not naturally lead to a conclusion that more spectrum should be allocated to utilities for the creation of a dedicated single use network for Smart Grid technologies. Wireless spectrum is a limited resource that must be utilized as efficiently as possible.[49]

Further, the Recovery Act requires the NBP to address the "most effective and efficient mechanisms for ensuring broadband access."[50] As AT&T has emphasized in these Comments, rather than allocate scarce spectrum to a small number of utilities for the construction of dedicated single use Smart Grid networks that are not positioned to expand broadband service to the public at large, spectrum should be allocated for use by commercial communications networks to meet Smart Grid needs in a more expedient and cost-effective manner. This approach enables "maximum utilization" of broadband infrastructure as Congress intended in the Recovery Act. It also encourages commercial communications operators to further extend broadband access to rural unserved areas if those areas contain electric grid infrastructure that must be served to accommodate a Smart Grid deployment.

---

[49] "One focus of the commission's attention over the next year will be looking at spectrum availability, and considering ways to ensure that all spectrum bands are being put to their highest and best use." *Communications Daily*, p. 5 (Sept. 16, 2009) (B. Gottlieb, Aide to FCC Chairman Genachowski).

[50] Recovery Act, Sec. 6001(k)(2)(A).

Allocating additional spectrum for the building of a dedicated single use network would also unnecessarily delay the deployment of the Smart Grid. A utility implementing its own private network over dedicated spectrum would have to clear the spectrum of incumbent users, design the Smart Grid network, negotiate with vendors to supply equipment, obtain permits (where needed) to erect antennas, and, of course, actually build the network. Each of these steps requires substantial time and more than a little uncertainty. Rather than undertake this time consuming and costly process, utilities and their customers would be better served by partnering with commercial communications operators to offer robust Smart Grid solutions with high standards of performance at a more economical cost.

f. Is additional spectrum required for Smart Grid applications? If so, why are current wireless solutions inadequate?

Comments: See AT&T's response to Question 3.e.

4. Real Time Data

b. What are the methods by which consumers can access this data (e.g., via Smart Meter, via a utility website, via third-party websites, etc.)? What are the relative merits and risks of each method?

Comments: While Smart Grid deployments are just beginning in the U.S., AT&T expects that, over time, Smart Grid technologies will provide consumers with access to two basic types of data: (1) near instantaneous pricing data to inform decisions about energy consumption; and (2) time-series data to analyze trends in energy usage. The methods by which customers would access this data are not yet established, but there are likely to be multiple options for the customer, depending on the application (website, phone, etc.). For example, future Smart Grid technologies may act as a portal into the home and would interconnect with home area networks or gateways that allow consumers to obtain real time energy consumption data; control home appliances; establish rules for energy consumption; and allow utilities to remotely manage devices under previous agreements with customers. In such an environment, pricing data could be used to trigger a change in energy usage based upon pricing or usage thresholds preprogrammed by the customer or the utility at the customer's request. It could also involve a real time arrangement whereby the customer is queried by their cell phone or an e-mail message as to whether a change in energy usage is desired. As Smart Grid technology matures, numerous other uses and applications will likely be developed.

c. How should third-party application developers and device makers use this data? How can strong privacy and security requirements be satisfied without stifling innovation?

Comments: The implementation of Smart Grid technologies to create a portal into the home to manage energy use also creates a potential opportunity for disclosures of customer information on energy usage and preferences. While this type of usage information has not been categorized for regulatory purposes, customers will likely view the information as "personal" – just as personal as their phone records. Privacy and security concerns may be heightened by fears that a hacker could access information about household energy consumption and preferences, which may result in the improper disclosure of personal information (e.g. when a family is away for an extended time) that might invite criminal activity.

To ensure Smart Grid acceptance and success, consumers will need to feel comfortable that their energy usage and preference information is protected. Security and privacy safeguards for household energy information will be needed to bring this level of comfort. Utilities and commercial communications operators providing connectivity to the Smart Grid will need to develop comprehensive policies for protecting energy information, including how information is collected, the manner in which the information is used, the appropriate persons or entities with which the information is shared, and the appropriate uses of that shared information.

Smart Grid customers will need to receive transparent disclosures of the energy information protection policies adopted by the commercial communications operators supporting their Smart Grid network. Further, utilities and commercial communications operators should disclose the manner in which they will use customer information to deliver and improve Smart Grid services. If the policy proposes the use of energy usage and preference information for marketing purposes, or any other purpose not directly related to the provision of energy, the customer should be given a reasonable opportunity to restrict the use of such information.

5. Home Area Networks.

a. Which types of devices (e.g., appliances, thermostats, and energy displays, etc.) will be connected to Smart Meters? What types of networking technologies will be used? What type of data will be shared between Smart Meters and devices?

Comments: Advanced Smart Grid devices are just now being introduced into the electric grid. NIST is still considering the standards for Smart Grid networks and devices, and the interaction between Smart Grid devices is still uncertain. Thus, it cannot be assumed that smart meters will be the primary control device for home area networks. In fact, it is more likely that the smart meter will be only one of many devices, along with appliances and thermostats, which are controlled by an intermediate server that manages the home area network. Smart meters should be adaptable to interacting with such an intermediate server rather than being designated as the device of choice for controlling in-home devices. To do otherwise would limit innovation needlessly.

Once a home area network is established, any device that uses electricity will be a candidate for networking within the home, including kitchen appliances, pool pumps, lights, vehicle charger interfaces, and air conditioning units. The basic data exchange from and to the utility and the basic information required to monitor and control the home area network should be standardized to encourage application development.

b. Which types of devices (e.g., appliances, thermostats, and energy displays, etc.) will be connected to the Internet? What types of networking technologies will be used? What type of data will be shared between these devices and the Internet?

Comments: Two types of data are likely to be available with a home area network – real time decision making data and aggregate, time-series consumption data. Real time decision making data would require security and immediate exchanges of query response transactions, such as for activating and deactivating devices connected to the network, based on price signals from the utility. Aggregate consumption data would potentially be provided in a dashboard type format, displaying cumulative consumption by device or family of devices and allowing the user to understand the devices that are driving household energy consumption.

In both cases, substantial security and privacy protections would need to be present to ensure that connecting such devices to the Internet does not result in the unauthorized disclosure of customer data. Thus, for example, a home server/gateway with accompanying security protections (e.g., a firewall), might provide an interface with the appliances and other devices connected to the network. The connections between the appliances and the home server/gateway are not likely to require substantial bandwidth given the relatively small amounts of data they will likely send to and receive from the server/gateway.

III. CONCLUSION

As the Smart Grid evolves and demand for network connectivity increases, utilities can leverage new network technologies deployed by commercial communications operators and optimize their network strategies and Smart Grid applications deployments.[51] This liberates utilities from the burden of building and managing their own networks and allows them to concentrate on new services for the consumer, optimizing energy utilization within the existing electrical grid, and implementing new information technologies that will allow utilities to enhance billing, customer relationships, demand response and management systems and energy management systems. Those benefits will be the true legacy of the Smart Grid.

[51] This process works in reverse as well, as added demand for broadband applications to support Smart Grid needs will help expand broadband availability.

Respectfully submitted,

Robert Vitanza
Gary L. Phillips
Paul K. Mancini

AT&T Inc.
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036
(202) 457-3076 – phone
(202) 457-3073 – facsimile

Its Attorneys

October 2, 2009